Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	1 MB
E-mail Remetente	**Hash da Mensagem**
rsidinei@gmail.com	d1a219a9099aa09c8e57a2d268ca72b9

Data de Envio	Assunto do E-mail	Anexos
30/07/2025 13:19:40	.Notificação de Cortesia_ref:doc expediente ACV-	Contém anexos

Evidências do Destinatário: gaspar.familia@tjsc.jus.br

Data/Hora Processamento	Evidência
30/07/2025 13:19:57	Entrega ao Servidor de email iCarta.
30/07/2025 13:19:57	Hash da mensagem iCarta: d1a219a9099aa09c8e57a2d268ca72b9
30/07/2025 13:19:57	Hash da mensagem iCarta do destinatário: 54e593e01b005a9b637e0149c6a88b10 .
30/07/2025 13:19:57	Assinatura DKIM: a=rsa-sha256; b=lPsWKcKz8uG8QImRqTsjWZFwbBGrkkzKCp6rhiHB8rmCnnkfzNC4iNY0BhKilUea3Uf O3sP6xllKnT8DPoR4e+XU+u2qF3PPNDv6VaF5bsX3nZuT3RUioPKN2VVqArwcJloTCqk ZvmYxLwWtQCzmPmLTAIcNVDowj0FRHbYToic=; s=dkim; c=relaxed/relaxed; d=icarta.pro; v=1; bh=azJU206YS4ahgCaK6PHXD8Icrt9NtIAjX46wIrK88iM=; h=From: To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding; .
30/07/2025 13:19:57	Aposição do Carimbo do Tempo (PLURIO), HLB(Hora Legal Brasileira): 30/07/2025 13:19:57.8 HLB GMT-03:00 destinatário: gaspar.familia@tjsc.jus.br
30/07/2025 13:19:58	Processo finalizado para o envio ao destinátario gaspar.familia@tjsc.jus.br .
30/07/2025 13:20:01	Início da tentativa de entrega às 2025-07-30 13:20:01 DEBUG: getProvider() returning javax.mail.Provider[TRANSPORT,smtp,com.sun.mail.smtp.SMTPTransport,Oracle] DEBUG SMTP: useEhlo true, useAuth false DEBUG SMTP: trying to connect to host "18.208.22.79", port 25, isSSL false 220 inpre01.tmes.trendmicro.com ESMTP Trend Micro Email Security DEBUG SMTP: connected to host "18.208.22.79", port: 25 EHLO smtp1.icarta.pro 250-inpre01.tmes.trendmicro.com 250-PIPELINING 250-SIZE 157286400 250-ETRN 250-STARTTLS 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-SMTPUTF8 250 CHUNKING DEBUG SMTP: Found extension "PIPELINING", arg "" DEBUG SMTP: Found extension "SIZE", arg "157286400" DEBUG SMTP: Found extension "ETRN", arg "" DEBUG SMTP: Found extension "STARTTLS", arg "" DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg "" DEBUG SMTP: Found extension "8BITMIME", arg "" DEBUG SMTP: Found extension "SMTPUTF8", arg "" DEBUG SMTP: Found extension "CHUNKING", arg "" STARTTLS 220 2.0.0 Ready to start TLS EHLO smtp1.icarta.pro 250-inpre01.tmes.trendmicro.com 250-PIPELINING 250-SIZE 157286400 250-ETRN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-SMTPUTF8 250 CHUNKING

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Perícia Técnica

Nome Remetente	Tamanho da Mensagem
FELIPE RUAN HORT	1 MB
E-mail Remetente	**Hash da Mensagem**
rsidinei@gmail.com	d1a219a9099aa09c8e57a2d268ca72b9

Data de Envio	Assunto do E-mail	Anexos
30/07/2025 13:19:40	.Notificação de Cortesia_ref:doc expediente ACV-	Contém anexos

DEBUG SMTP: Found extension "PIPELINING", arg ""
DEBUG SMTP: Found extension "SIZE", arg "157286400"
DEBUG SMTP: Found extension "ETRN", arg ""
DEBUG SMTP: Found extension "ENHANCEDSTATUSCODES", arg ""
DEBUG SMTP: Found extension "8BITMIME", arg ""
DEBUG SMTP: Found extension "SMTPUTF8", arg ""
DEBUG SMTP: Found extension "CHUNKING", arg ""
DEBUG SMTP: use8bit true
DEBUG SMTP: found an 8bit part
MAIL FROM:<0ba3b130-7050-4532-a9e2-85d897cfe599-pid@icarta.pro>
250 2.1.0 Ok
DEBUG SMTP: sendPartial set
RCPT TO:<gaspar.familia@tjsc.jus.br>
250 2.1.5 Ok
DEBUG SMTP: Verified Addresses
DEBUG SMTP: gaspar.familia@tjsc.jus.br
DATA
354 End data with <CR><LF>.<CR><LF>
.
250 2.0.0 Ok: queued as 6AB261008AA89
DEBUG SMTP: message successfully delivered to mail server
QUIT
221 2.0.0 Bye

Mensagem entregue às 2025-07-30 13:20:01
.

* DKIM é uma especificação do IETF que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas. Através do uso do DKIM, uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem. Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.